Interoperability of heterogeneous distributed systems

Zaschke, C., Essendorfer, B., Kerth, C.
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe, GERMANY
christian.zaschke@iosb.fraunhofer.de, www.iosb.fraunhofer.de

ABSTRACT

To achieve knowledge superiority in today's operations interoperability is the key. Budget restrictions as well as the complexity and multiplicity of threats combined with the fact that not single nations but whole areas are subject to attacks force nations to collaborate and share information as appropriate.

Multiple data and information sources produce different kinds of data, real time and non-real time, in different formats that are disseminated to the respective command and control level for further distribution. The data is most of the time highly sensitive and restricted in terms of sharing. The question is how to make this data available to the right people at the right time with the right granularity.

The Coalition Shared Data concept aims to provide a solution to these questions. It has been developed within several multinational projects and evolved over time. A continuous improvement process was established and resulted in the adaptation of the architecture as well as the technical solution and the processes it supports.

Coming from the idea of making use of existing standards and basing the concept on sharing of data through standardized interfaces and formats and enabling metadata based query the concept merged with a more sophisticated service based approach.

The paper addresses concepts for information sharing to facilitate interoperability between heterogeneous distributed systems. It introduces the methods that were used and the challenges that had to be overcome. Furthermore, the paper gives a perspective how the concept could be used in the future and what measures have to be taken to successfully bring it into operations.

Keywords: Interoperability, CSD, Coalition Shared Data, information, distribution, sharing, standard, metadata

1. INTRODUCTION

The conflicts and disasters of the last years have shown a high demand for quick and flexible solutions for problems that require cooperation between different organizations and nations. Conflicts changed dramatically and more and more nations are being confronted with a vast number of possible threat scenarios. Key challenges identified by [1] are terrorism, hostile, fragile and failing states, hybrid threats, globalization as well as environmental and humanitarian topics.

In the last two decades globalization has created complex economic and sociologic dependencies. Modern communication technology enables the dissemination of data and information in near real-time and creates the ability for both aggressors and defenders to act remotely and to network over time and space. Technological development with respect to sensors and platforms as well as network technology and storage capability has evolved and mass data can be easily shared and disseminated.

To make use of these new capabilities, there is a need for systems that are able to interact with each other in a well-defined way. The basis of creating such interoperable systems are compatible interfaces for data exchange and the ability to interpret the disseminated data in a correct manner.

As an example, the refugee crisis in Syria with its implications for Europe and the whole world revealed a noticeable lack of interoperability even in technologically advanced nations like Germany. Different responsibilities and incompatible computer systems [2] prevent up-to-date and efficient acquisition, processing and exchange of data. As a consequence, data has to be entered manually several times by different authorities and departments [3] which results in significantly increased efforts and longer processing times.

Budget restrictions as well as the fact that not single nations but socioeconomic alliances are subject to threats and have to meet the economical, ecological and humanitarian challenges demand collaboration between both civil and military organizations. Flexible means to collaborate and share resources, applications and information need to be developed.

Knowledge superiority is more and more a question of being able to get the right information to the right person at the right time for enabling the right decision and the right conclusions. The German police, for example, has also identified that availability of information and interoperability between distributed systems of other departments and even other nations is a key factor for successfully fulfilling their complex tasks. Therefore it has introduced a modern, highly available and extraordinarily efficient IT infrastructure [4]. It allows the operation of shared IT procedures and facilitates the interoperability with international information systems.

This paper reflects on the mentioned aspects and describes a method and the technological basis to share data and, resulting from it, information in heterogeneous coalitions. Coming from a military context the described concepts and technologies also apply to the civil environment as the requirements are very similar.

The next chapter defines the basic terms and points out the high level requirements for sharing data in a common environment. In Chapter 3 the concept of Coalition Shared Data is described in more detail and the evolution of the concept over the last decade is highlighted. The application of the concept and challenges therein are pointed out in Chapter 4. Finally a conclusion and further steps are detailed.

2. INFORMATION SHARING IN A HETEROGENEOUS DISTRIBUTED ENVIRONMENT

Knowledge superiority in today's military and civil security operations is provided by the ability to get the right information to the right person at the right time. As technology and personnel supporting these operations are provided by multiple organizations and even nations, it is of interest to specify the processes that are supported and to identify the interfaces where information is passed from one system to another.

Interoperability is a vital and time critical aspect here. As already specified in [5], interoperability is understood as the ability of systems, organizations or discrete parts of the same organization to provide metadata and information to and accept metadata and information from other systems, organizations or discrete parts of the same organization, and to use the metadata and information so exchanged to enable them to operate effectively together [6].

Clearly different aspects have to be taken into account to achieve interoperability. In literature there are different approaches to specify different levels of interoperability. In this paper the levels of technical, syntactical, semantic and pragmatic interoperability are described (Level 1-4 from [7]).

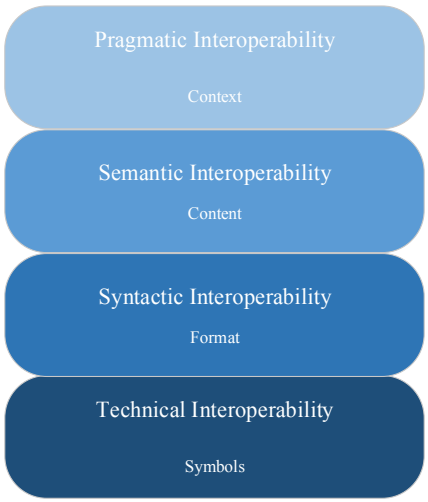

Figure 1: Interoperability levels

Technical aspects deal with the physical connections, the protocol layer and the symbols that are exchanged.
The syntactic layer defines the structure of data and deals with the format. The semantic layer models and conceptualizes the content of information. Knowledge interoperability (represented in the pragmatic interoperability layer in Figure 1) is achieved through a common understanding visualized in a common operational picture and leads to common situational awareness. The lower levels of interoperability can be achieved by technical definitions, whereas the more complex aspects of interoperability need harmonization of organizational structures as well as a common understanding between the individuals that interact. The context must be understood. Thus pragmatic interoperability that addresses aligned procedures, operations, strategies and doctrines as well as high level objectives is the most complex aspect and hard to achieve especially in operations where heterogeneous forces and organizations have to interact with each other (see also [8]). Here cultural (organizational and/or ethnical), sociological and psychological aspects have to be taken into account and need to be explicitly understood (see also [9]).
Higher level interoperability relies at least partially upon interoperability on the lower levels.

The focus of this paper lies on the lower interoperability levels with a clear aim to support pragmatic interoperability. In the following sections, the core aspects of interoperability for security operations are outlined and requirements are derived.

2.1 Interoperability in security operations

In this paper the term “security operations” shall cover all kinds of operations that focus on the continuation, stabilization or recovery of public security. Threats for public security can be natural or man-made disasters (or a combination of both), (terrorist) attacks on network, transportation, public areas and borders, as well as uncontrolled border crossing, smuggling and trafficking. Depending on the type of threat this can be on a national, union or international level.

The more complex a threat is, the higher is the number of organizations that will be part of such a security operation. As each organization has its own assets and defined processes they work with, data and information interoperability and common interfaces to exchange information are necessary to collaborate.

In an environment where different military forces cooperate within a coalition, intelligence and reconnaissance data is passed on through Joint ISR (Intelligence, Surveillance and Reconnaissance) and the Intelligence Process Cycle. Specifics of this process are defined in [5].

In civil security operations, forces such as border protection units, the police, firefighters, ambulances and government organizations collaborate with each other. Depending on the type of threat, these collaborations might be well planned or ad hoc. A difficulty here is, that these organizations often act and are funded locally and monetary investment in modern technology or information exchange processes is very low, resulting in a lack of coordination possibilities.

In civil-military co-operation (CIMIC), for example when restoring public security after a military conflict, the above mentioned forces have to collaborate and very different processes as well as technology (levels) have to be aligned.

Common to all those operations are highly specialized forces and systems (this refers to technology and processes) which have to collaborate and exchange information. Especially in military organizations the hierarchies and the connected roles, tasks and rights have to be obeyed. In most security operations time plays an important role. Information has to be passed on quickly to enable decision makers to enforce the right reaction. Not all information can be openly passed on to achieve knowledge superiority and subsequently react correctly – some information is sensitive and must be protected.

As already stated above, a difference is that military organizations are funded nationally and thus financial investment in interoperability projects and networks are possible, sometimes even across nations. In contrast, civil security organizations are most of the time funded locally or on federal state level, which results in the lack of investment in overarching projects and networks.

2.2 Requirements

From the previous chapters, it is clear that operational needs have to be taken into account when sharing data in security operations.

Detailed requirements have to be defined for individual settings, but exemplary high level requirements can be defined here. The requirements are derived from current military doctrine and guidance in this domain (see [10] and [1]) as well as from civil operations [11]. It has to be taken into account that some requirements might be difficult to fulfil especially in civil or CIMIC operations (see above).

Especially in military and joint civil and military operations, *security aspects* are of high relevance. As already defined in [5] this includes the ability to support data and information classification, releasability and policies. Especially when multi-domain security is of relevance and different nations are sharing data, those aspects need to be taken into account. A technical solution has to support data and information tagging according to classification, releasability and policy, auditing and eventually cross domain security.

Clear syntactic and semantic definitions to make sure that information that is released by one operational unit is also understood by the receiving operational unit are essential. As *interpretability* is not only subject to syntactic definitions but also to semantics, linguistic aspects are of relevance here. To be able to operate across borders and different mother tongues a common language (e.g. English) is used to collaborate. This can lead to linguistic fuzziness. Cultural aspects as well as background knowledge influence the way one perceives the world (see [12]) which in turn influences how the information is interpreted. Not only clear definitions and documentation must be available, collaborative training to enforce better mutual understanding must also be provided. On a technical level, this means that not only pure data but also metadata has to be provided, to enable cataloguing and querying as well as the interpretation where, when and by whom the data was collected.

The information received itself must be *reliable* (not manipulated or fragmented) and the source must be *credible*. On a technical level this means that data must be labelled according to its source and the reliability of this source. Especially in CIMIC this requirement is difficult to fulfil as civilian communication infrastructure is often failure-prone [11].

Timeliness is also relevant in an environment, where quick reaction to an event is often making the difference between success and failure. This has to be seen in connection with the fact that operational networks do have limitations in bandwidth and availability. Dealing with these network limitations is also an important aspect. Data dissemination needs to respect network specific aspects such as local vs. wide area network (depending on where the data has to be disseminated to), bandwidth restrictions (data rate and availability) as well as network types.

In general, information needs to be available for the right person at the right time in the right abstraction. This also means that operational processes must be observed and understood. Cooperation between different organizations does not occur on its own but must be constructed and learned, to avoid confusion and minimize response times. This includes the knowledge of the expert level and tasking of personnel throughout the information chain (what is of relevance, which information might be neglected that still is of relevance in a later process step). User roles and preferences also need to be supported by technical means. This refers to the ability to filter data based on its attributes (e.g., security attributes, types, reconnaissance levels).

Further non-functional requirements as *usability, efficiency, maintainability and portability* (see [13]) also have to be supported. Portability especially points to the fact that solutions have to be vendor independent and thus standards on data

and information level as well as on system level are important in an environment where many organizations and thus technology from many different vendors interact.

3. COALITION SHARED DATA CONCEPT

To achieve the requirements described in Chapter 2.2 the Coalition Shared Data (CSD) concept is of interest. It has its origin in multinational military-oriented projects. Although the community, workflows and specific data formats differ between the civilian and the military environment, the underlying principals apply to both.

The concept of Coalition Shared Data first started with the sharing of fixed, finished data such as reports, images and video clips. Over time the scope was extended with the ability to share mutable data – such as we can encounter in collaborative business processes where multiple parties modify a common piece of data – and ever changing data such as live video streams. As the scope grew, the amount of requirements on the systems increased, too. The approach of feeding all data through a single system type revealed serious weaknesses, especially as the diverging types of data required different forms of representation as well as different mechanisms to search and interact among participants. This lead to the evolution of the Coalition Shared Data from a client-server architecture towards a service-oriented, multi-layer service set. This evolution is described in more detail in Chapter 3.2 “Evolution of the CSD architecture”.

Coalition Shared Data is a technology agnostic concept. Contrary to being a specific solution, its aim is to share data within a coalition, i.e. among a set of participants that are interacting with each other. The concept is based on having a network of physically distributed sites, connected using the available network infrastructure. Among the sites, each node shares information about the persisted content using metadata entries. By distributing the metadata across all instances of participating sites using adequate synchronization protocols, a global awareness of available data is achieved. Combining such awareness with the ability to retrieve files on demand, enables ubiquitous access capabilities for data stored on any of the sites in the entire network with reduced network traffic [14].

As the concept itself was defined within a military-oriented environment the original setting of CSD is Joint ISR. Naturally the concept and its technological approach could also be applied for resembling environments and/or civilian environments that have similar requirements.

Within Chapter 2 the mentioned major aspect is interoperability and the levels of interoperability that need reflection. This means, that the development of a solution requires incorporation of data, information and knowledge sharing alike.

In the coming sections, the main architectural development principles are outlined. The principles guided the transformation from the pure concept into a specific technological solution.

3.1 Architectural development principles

3.1.1 Multinational collaboration

The projects which underpinned the development of both the CSD concept and its technical solution were of multinational nature. As each nation brings its own approach and provides a subset of the assets forming the complete coalition, the aspects of interoperability within a coalition are respected.

Through national contributions to the Intelligence and Reconnaissance Cycle, numerous national data sources (i.e. sensors and intelligence sources) are made available to the whole community. The data that was produced through these national assets is then processed through additional national capabilities (i.e. ground stations, exploitation stations) and disseminated using national systems that obey national rules and processes.

Connecting these national assets belonging to different nations and using them together is the real challenge. This challenge is practically tackled by ensuring participation of as many nations as possible in the collaboration.

3.1.2 Collaboration between operational and technical experts

The technical architecture depends on the operational constraints outlined in Chapter 2. Further, for the task outlined by the constraints, expectations exist by the operational personnel. To be able to achieve success, a close collaboration between the technical experts – that are responsible for identifying and building the technical solution – and the operational experts – that best know the requirements and the target domain – needs to be established. Complementary to the collaborative work on the solution itself, it is then possible to perform expectation management in both directions.

Such an approach has the positive side-effect of the system being known and understood by operational personnel before it is even deployed. The risk of missing user acceptance is mitigated by operational experts pushing their knowledge to colleagues and the thus widened community can provide additional proposals to be incorporated by the technical experts.

3.1.3 Software development process model

In order to achieve their project goals, the spiral model was applied throughout the research and development projects. The cycles where implemented using exercises where software from different vendors were connected to enable identification of remaining issues (termed risks according to [15]). Subsequent collaborative prioritization and the following selection of the most pressing risks then fed into the next spiral of the process and solution maturity.

3.1.4 Usage of standards, reference architectures and taxonomies

The multinational projects which developed and enhanced the CSD concept made use of available standards and standard definitions wherever possible and applicable. This is true on operational level as well as on architectural level.

Originating from a military environment, it relied heavily on NATO Standardization Agreements (STANAGs). The standards used included STANAG 4559 [16] for data sharing, STANAG 4545 [17] for imagery, STANAG 4609 for motion imagery, STANAG 3377 / 3596 and STANAG 2433 (HUMINT / PENTAGRAMREP) for reporting and STANAG 4607 for radar data.

When applying the CSD concept to civilian environments, some of the standards might not be applicable as different types of data/information are being used. Other standards might be used to complement or even supersede the military standards as available systems are already built towards industry standards. Candidates for industry standards could be:

- OGC Sensor Web Enablement (SWE) [18],
- Electronic Business Registry Information Model (ebRIM, ISO 19135) [19],
- ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange; standard for air traffic control) [20].

3.2 Evolution of the CSD architecture

3.2.1 Client-server based architecture

As outlined at the beginning of Chapter 3, the CSD architecture began with a single type of storage server that was responsible for the durable persistence of all data. Tasking data, sensor data, exploitation and streaming were all stored in a single type of system, despite their diverging update rates, sizes and need for local/global modification needs. This architecture reflected the client-server architecture that enabled ubiquitous availability of metadata with the possibility to gain access to the files referenced in the metadata on demand.

Retrieving the reference files was supplemented by preview files that allowed the user to get a glance at the data before he requested the entire – potentially large – file. To reduce the burden on the network further, the user could request only sections of the entire file to prevent the unnecessary transmission of file content he did not need to complete his task (e.g., cropped imagery data).

By doing so, the CSD architecture was able to provide network-friendly access to large files. As its design originates from static data, it imposed drawbacks for the other types of data:

- Overhead of metadata for continuously changing data elements (e.g., streaming data) that resulted in either untimely availability of information or a poor abstraction in query results.
- Missing support for modification of data across multiple servers, thus prevented operational requirements such as collaborative updates to tasking.

The adaptation of the architecture to provide adequate support for all types of data led to a shift that replaced the two-layer architecture containing a single server with a multi-layered architecture consisting of specialized services and dissemination capabilities.

3.2.2 Multi-layer based Service Oriented Architecture

Performing incremental improvements on the architecture, multiple additions and migrations of responsibilities were done over the course of years. Doing so provided backward compatibility with prior versions of systems and the standards they implement. With the necessary migration of responsibility, new systems were introduced into the architecture that better suit the job than the previous components. Over time, more and more of the limitations identified for the client-server architecture were resolved.

Once the separation of concerns on the persistence layer was completed, the architecture featured three different types of systems instead on just one:

1. Storage for static data,
2. Storage for data subject to ongoing modifications (e.g., tasking information),
3. Storage for streamed data (e.g., video streaming)

Storage type (1) resembles the original storage type before dynamic and streaming data were added to the architecture. Hence, its synchronization protocol remained unchanged over time. However, the storage types (2) and (3) are – depending on the specific data element and process steps they are used in – subject to global modification needs. Therefore, replication protocols have been developed to enable an exchange of data belonging to the storage types (2) and (3).

In addition to the separation of the storage concerns, further services were introduced between the clients and the storage system to factor out business logic where needed. By adding more validation logic and cross-checks spanning multiple data elements, these new services steered towards improved information quality and automated compliance checks for information elements with defined procedures and policies.

3.3 Challenges and solutions

With the separation of storage and processing responsibilities on multiple systems, the number of systems that require fielding and maintenance rose. With dependencies between the systems, one issue is the increased probability of parts of the set of systems being unavailable. Without mitigation, a high enough number of depending systems would reduce overall availability enough to render it operationally unusable.

To avoid the problem from resulting in continuous outages of the architecture, the individual components were equipped with compensation mechanisms that achieve light coupling whilst keeping the needed performance at a reliability level that is high enough.

Another challenge was and still is the compatibility of the evolved architecture with existing operational systems that are in active usage. Even though this task was simplified by retaining standards for interfaces, changes to the storage formats and separation of storage responsibility imposed the need to map the evolved architecture with its predecessor versions. Some parts can be mapped with automated rules, e.g., where the shared information is the same with only its representation format being different. Other cross-version problems needed to be compensated at higher levels by introducing “hybrid” systems that are able to operate in both worlds (old and new versions of the architecture), enabling interoperability directly on the operational level.

4. APPLICATION OF THE COALITION SHARED DATA CONCEPT

In a world where nations and organizations need to collaborate to meet the complex security challenges the CSD concept is of interest in a variety of environments. As the concept can be adapted to include other security standards and add other COI (community of interest) specific services, civil security or CIMIC operations could benefit from it. The following sections aim to point out a potential subset and describe how current problems could be solved using the CSD architecture.

4.1 Interoperability in public administration

Interoperability in the civil security sector is a topic for very different applications. With its ability to connect different network nodes (that itself are under the control of the respective (national) organizations) metadata-based exchange of

datasets is possible. As connecting domains with different security classification is a well-known problem and solutions using specific gateways exist, tailored information exchange is possible.

This could be of interest when exchanging data between administrative units of nations (for example when moving to another country in the EU [21]) or between different national department units (for example when passing on refugee information between federal state administration (see Chapter 1)).

By defining common formats, transmission mechanisms and processes, the burden of necessary paperwork would be diminished. Limitations imposed on information sharing (e.g., by laws) would need to be taken into account by selectively sharing the information that is both necessary and permitted to be transferred among participants, resulting in the availability of the relevant information. In addition to resolving the need for duplicated manual labor, the CSD architecture can serve as a foundation for optimizing the process itself and including further automated mechanisms.

4.2 Interoperability in CIMIC operations

In CIMIC operations (as depicted in Chapter 2.1) the CSD concept can be used to connect the military domain with the civilian security sector.
As pointed out in Chapter 3.1.4 the military standards can be supported by civilian standards.
A bridging system could provide an interface that conforms to a military standard to connect to a military network and an interface that conforms to a civilian standard to connect to a civilian security node.
As pointed out above, solutions for different security domains exist. Thus, data labeling and filtering is possible.
In a scenario where civil surveillance systems provide their data to a military surveillance unit or a common operational picture is passed on between civil and military organizations, the CSD concept would enable information exchange. In regions where civil communication networks are limited (see [11]) available military network could be used to "transport" civilian data and enhance overall situation awareness.

4.3 Interoperability in civil security operations

Not only within each nation but also across nations interoperability is of high importance. In a harbor protection scenario the CSD principle could be used to connect sensor and exploitation systems from different vendors by using common interfaces and defining and using common data formats. Data translation services could be established to translate proprietary formats to common ones. As data collected in one harbor could be of interest in other harbors (along a shipping route) the CSD concept can be used as well to connect those different sites (and nations) and exchange data adequately. An example for the application of this concept in such a scenario is given in [22].

As an example for successful interoperability, the Interpol network and databases can be named, where the need for interoperability is a challenge at hand [4]. With its international collaboration, Interpol has achieved interoperability across police forces using standardized communication, consistency checks, adaptable input forms for structured information and real-time access to the relevant information [23].

This example also highlights national security concerns: the Interpol network is spread across multiple nations, each imposing its own legislative rules on the system being used. With the right approach, it is possible to operate a distributed system that is connecting the 190 participating countries [21].

5. CONCLUSION AND FURTHER WORK

The CSD concept has already proved its efficiency in NNEC (NATO Network Enabled Capability) operations for the forces in the military sector. And as the conflicts and disasters of the last years have shown, there is a need for interoperability in the civil sector [2] and in the civil-military co-operation, too. Information that is generated in a civil context could be of interest for military users and vice versa. In case of emergencies, for example, it may be useful for civil authorities and organizations to use military capabilities to avert serious damages.

As the requirements in the civil and military security domain are similar, the CSD concept could help with solving compatibility issues between authorities and organizations that need to share information. With changing the application area, new challenges like the failure-prone civilian communication structure [11] and data protection regulations arise. Data protection and security concerns can be handled analogical to the security topics in the military domain and are

therefore not critical. Error handling mechanisms and fault tolerant systems and processes could help to cope with fault-prone communication channels.

More difficult is the handling of the processes and workflows within or between civil actors which leads to a higher effort on establishing interoperability on a semantic or even pragmatic level. Thus, the negotiation and definition of standardized protocols, interfaces and formats to ensure interoperability on a technical level should be done beforehand by interoperability experts and potential users. After that, the advantages of systems which follow those standards should be advertised and communicated to other potential users to gain acceptance and agreement and to achieve a continuous propagation.

Another difference between the military and the civil sector is the financing. Organizations like police, firefighters and medical authorities are normally funded locally or on a state level and not on a federal level. This results in a lack of investment in new technology and overarching processes. Hence, dual use has to be enforced and could help to deal with this problem. Technology developed in a military context has to be adapted to react more flexibly on specific civil demands and civil security operations requirements. More research should be invested in comparing these requirements based on exemplary operations. Because in the civilian sector investment in overarching interoperability projects is unlikely, research has to be invested in existing interfaces and formats (on civilian side), as well as flexible adapters between civil and military standards to be able to easily connect civil security systems and military systems.

ACKNOWLEDGMENT

The CSD concept is part of multinational projects that were funded by the BMVg (Federal Ministry of Defence). The authors acknowledge valuable help and contributions from all partners of the projects.

The authors would like to thank their colleagues and students, who have contributed to the work presented in this paper, especially Daniel Haferkorn, Achim Kuwertz and Jennifer Sander.

REFERENCES

[1] NSA, "AJP-2 (A) ALLIED JOINT DOCTRINE FOR INTELLIGENCE; COUNTER-INTELLIGENCE AND SECURITY. Study Draft 1 - Version 1", (2012).

[2] Berliner Morgenpost, "Flüchtlinge – Deutschlands Ämter arbeiten ineffizient", 23 August 2015, <http://www.morgenpost.de/politik/article205594913/Fluechtlinge-Deutschlands-Aemter-arbeiten-ineffizient.html> (Accessed: 04 March 2016).

[3] ZEIT ONLINE, "Warten auf „Aktenanlage“ verlängert Asylverfahren", 10 October 2015, <http://www.zeit.de/politik/deutschland/2015-10/asylverfahren-fluechtlinge-bamf-erstaufnahme> (Accessed: 04 March 2016).

[4] Bundeskriminalamt, "Abteilung „Informationstechnik“ (IT)", 2016, <http://www.polizei.de/DE/DasBKA/Organisation/IT/organisationIT__node.html> (Accessed: 04 March 2016).

[5] Essendorfer, B., Kerth, C., Zaschke, C., "Evolution of the Coalition Shared Data concept in Joint ISR", IST-SET-126, (May 2015).

[6] Hura, M., "Interoperability: A Continuing Challenge in Coalition Air Operations", RAND, (2000).

[7] Wang, W.G., Tolk, A., Wang, W.P., "The levels of conceptual interoperability model: Applying systems engineering principles to M&S.", Proc. SpringSim'09, (2009).

[8] Wunder, M. and Grosche, J., "Verteilte Führungsinformationssysteme", Springer, (2009).

[9] Hofstede, G., "Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations", Thousand Oaks CA: Sage Publications, (2001).

[10] NAFAG, "AEDP-2. NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture", NATO, September 2005, <http://www.nato.int/structur/ac/224/standard/AEDP2/AEDP02.htm> (Accessed: 12 March 2015).

[11] Zdravković, M., Noran, O., Panetto, H., Trajanović, M., "Enabling Interoperability as a Property of Ubiquitous Systems for Disaster Management", Computer Science and Information Systems, Vol. 12, No. 3, 1009–1031 (2015).
[12] Jager Adams, M., Tenney, Y. and Pew, R., "Situation Awareness and the Cognitive Management of Complex Systems", Human Factors: The Journal of the Human Factors and Ergonomics, Nr. 37/1, 85-104 (March 1995).
[13] ISO, "ISO/IEC 25000:2014", 15 March 2014, <https://www.iso.org/obp/ui/#iso:std:iso-iec:25000:ed-2:v1:en> (Accessed: 13 March 2015).
[14] Essendorfer, B., Kerth, C., Schneider, G., "A Multilevel Approach to Interoperability in Surveillance and Reconnaissance", BIDW 2010 and DAMD 2010, (July 2010).
[15] Boehm, B. W., "Tutorial: Software Risk Management", IEEE Computer Society Press, 61-72 (1989).
[16] NSO, "STANAG 4559. Edition 3", NATO, November 2010, <http://www.nato.int/structur/AC/224/standard/4559/4559Eed03.pdf> (Accessed: 23 March 2015).
[17] MAS, "NATO Secondary Imagery Format (NSIF) ", NATO, November 1998, <http://www.nato.int/structur/ac/224/standard/4545/4545_documents/4545_ed1_amd1.pdf> (Accessed: 23 March 2015).
[18] OGC, "Sensor Web Enablement (SWE)", 2016, <http://www.opengeospatial.org/ogc/markets-technologies/swe> (Accessed: 11 March 2016).
[19] OASIS, "ebXML Registry Information Model Version 3.0", 02 May 2005, <http://docs.oasis-open.org/regrep/regrep-rim/v3.0/regrep-rim-3.0-os.pdf> (Accessed: 11 March 2016).
[20] EUROCONTROL, "ASTERIX", 2016, <http://www.eurocontrol.int/asterix> (Accessed: 11 March 2016).
[21] ISA, "Helping Europe move towards a digital single market", 2016, <http://ec.europa.eu/isa/about-isa/index_en.htm> (Accessed: 08 March 2016).
[22] Essendorfer, B., Monari, E., Wanning, H., "An Integrated System for Intelligence, Surveillance and Reconnaissance (ISR)", IARIA: International Journal on Advances in Security, Vol. 2, No. 2&3, 256- 266 (2009).
[23] Interpol, "I-link: taking data exchange to the next level", 2016, <http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-link> (Accessed: 08 March 2016).